

LATHAM & WATKINS LLP
Elizabeth L. Deeley (CA Bar No. 230798)
elizabeth.deeley@lw.com
505 Montgomery Street, Suite 2000
San Francisco, California 94111-6538
Telephone: +1.415.391.0600
Facsimile: +1.415.395.8095

Susan E. Engel (*pro hac vice*)
susan.engel@lw.com
555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Telephone: +1.202.637.2200
Facsimile: +1.202.637.2201

Serrin Turner (*pro hac vice*)
serrin.turner@lw.com
1271 Avenue of the Americas
New York, NY 10020
Telephone: +1.212.906.1200
Facsimile: +1.212.751.4864

Attorneys for Defendant Zynga Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

I.C., a minor, by and through his natural
parent, NASIM CHAUDHRI, AMY GITRE,
CAROL JOHNSON, LISA THOMAS,
JOSEPH MARTINEZ IV, DANIEL PETRO,
and CHRISTOPHER ROSIAK, individually
and on behalf of all others similarly situated,

Plaintiffs,

v.

ZYNGA INC.,

Defendant.

Case No.: 4:20-cv-01539-YGR

**DEFENDANT ZYNGA INC.'S REPLY IN
SUPPORT OF MOTION TO DISMISS
SECOND AMENDED CONSOLIDATED
CLASS ACTION COMPLAINT**

Hearing: October 26, 2021
Time: 2:00 p.m.
Location: Courtroom 1 – 4th Floor
Judge: Hon. Yvonne Gonzalez Rogers

TABLE OF CONTENTS

		Page
1		
2		
3	I. INTRODUCTION	1
4	II. PLAINTIFFS’ ALLEGATIONS BASED ON THE RISK OF FUTURE	
5	IDENTITY THEFT DO NOT PROVIDE A BASIS FOR STANDING.....	2
6	A. <i>TransUnion</i> Forecloses Any Standing Argument Based on a Risk	
7	of Future Harm.....	2
8	B. Plaintiffs Cannot Manufacture Standing Based on Mitigation	
9	Efforts or Emotional Distress Allegedly Stemming from the Risk	
10	of Identity Theft	5
11	1. Mitigation Efforts.....	5
12	2. Emotional Distress	6
13	C. Plaintiffs Cannot Establish Standing Based on an Alleged “Loss of	
14	Value” in Their Information	7
15	III. PLAINTIFFS FAIL TO ALLEGE ANY PRIVACY INJURY WITH A	
16	CLOSE CONNECTION TO A COMMON LAW TORT.....	9
17	A. Plaintiffs Fail to Allege an Injury with a Close Connection to the	
18	Tort of Publicity Given to Private Life	9
19	B. Plaintiffs Fail To Allege an Injury with a Close Relationship to the	
20	Tort of Intrusion Upon Seclusion	12
21	IV. PLAINTIFFS LACK STANDING FOR THEIR INJUNCTIVE RELIEF	
22	CLAIM.....	14
23	V. CONCLUSION.....	15
24		
25		
26		
27		
28		

TABLE OF AUTHORITIES**Page(s)****CASES**

<i>In re Anthem, Inc. Data Breach Litig.</i> , No. 15-MD-02617-LHK, 2016 WL 3029783 (N.D. Cal. May 27, 2016)	6
<i>Bass v. Facebook, Inc.</i> , 394 F. Supp. 3d 1024 (N.D. Cal. 2019)	8
<i>In re Blackbaud, Inc., Customer Data Breach Litig.</i> , No. 20-MN-02972, 2021 WL 2718439 (D.S.C. July 1, 2021)	4
<i>Burgess v. Eforce Media, Inc.</i> , No. 1:07-cv-231, 2007 WL 3355369 (W.D.N.C. Nov. 9, 2007)	14
<i>Busse v. Motorola, Inc.</i> , 813 N.E.2d 1013 (Ill. App. Ct. 2004)	13
<i>Chisholm v. Foothill Capital Corp.</i> , 3 F. Supp. 2d 925 (N.D. Ill. 1998)	10
<i>Clapper v. Amnesty Int’l</i> , 568 U.S. 398 (2013)	7
<i>Claridge v. RockYou, Inc.</i> , 785 F. Supp. 2d 855 (N.D. Cal. 2011)	8
<i>Davis v. Facebook, Inc. (In re Facebook Inc. Internet Tracking Litig.)</i> , 956 F.3d 589 (9th Cir. 2020)	11
<i>Dearing v. Magellan Health Inc.</i> , No. CV-20-00747-PHX-SPL, 2020 WL 7041059 (D. Ariz. Sept. 3, 2020)	8
<i>In re Equifax, Inc., Customer Data Sec. Breach Litig.</i> , No. 1:17-MD-2800-TWT, 2019 WL 926999 (N.D. Ga. Jan. 28, 2019)	6
<i>In re Experian Data Breach Litig.</i> , No. SACV151592AGDFMX, 2016 WL 7973595 (C.D. Cal. Dec. 29, 2016)	6, 8
<i>In re Facebook Privacy Litigation</i> , 572 F. App’x 494 (9th Cir. 2014)	8
<i>Fernandez v. Leidos, Inc.</i> , 127 F. Supp. 3d 1078 (E.D. Cal. 2015)	9

1	<i>Gadelhak v. AT&T Servs., Inc.</i> ,	
2	950 F.3d 458 (7th Cir. 2020)	14
3	<i>In re Google, Inc. Privacy Pol’y Litig.</i> ,	
4	No. 5:12-CV-001382-PSG, 2015 WL 4317479 (N.D. Cal. July 15, 2015).....	7
5	<i>Grauman v. Equifax Info. Servs.</i> ,	
6	No. 20-cv-3152, 2021 WL 3239865 (E.D.N.Y. July 16, 2021).....	4
7	<i>Hameed-Bolden v. Forever 21 Retail, Inc.</i> ,	
8	No. CV1803019SJOJPRX, 2018 WL 6802818 (C.D. Cal. Oct. 1, 2018)	8
9	<i>Hunstein v. Preferred Collection & Mgmt. Servs.</i> ,	
10	994 F.3d 1341 (11th Cir. 2021)	10, 11
11	<i>Ignat v. Yum! Brands, Inc.</i> ,	
12	214 Cal. App. 4th 808 (2013)	10
13	<i>Iwaniw v. Early Warning Servs.</i> ,	
14	No. 20-cv-5266, 2021 WL 3209856 (E.D. Pa. July 28, 2021)	4
15	<i>Jackson v. Loews Hotels, Inc.</i> ,	
16	No. EDCV18827DMGJCX, 2019 WL 6721637 (C.D. Cal. July 24, 2019).....	14
17	<i>Karimi v. Golden Gate Sch. of L.</i> ,	
18	361 F. Supp. 3d 956,980 (N.D. Cal. 2019), <i>aff’d</i> , 796 F. App’x 462 (9th Cir. 2020)	9
19	<i>Keller v. Northstar Location Servs.</i> ,	
20	No. 21-cv-3389, 2021 WL 3709183 (N.D. Ill. Aug. 20, 2021)	11
21	<i>Krottner v. Starbucks Corp.</i> ,	
22	628 F.3d 1139 (9th Cir. 2010)	5, 6
23	<i>Lewert v. P.F. Chang’s China Bistro, Inc.</i> ,	
24	819 F.3d 963 (7th Cir. 2016)	6
25	<i>In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.</i> ,	
26	440 F. Supp. 3d 447 (D. Md. 2020)	8
27	<i>O’Shea v. Littleton</i> ,	
28	414 U.S. 488 (1974).....	14
	<i>Oppenheim v. I.C. Sys., Inc.</i> ,	
	695 F. Supp. 2d 1303 (M.D. Fla.), <i>aff’d</i> , 627 F.3d 833 (11th Cir. 2010)	14
	<i>Razuki v. Caliber Home Loans, Inc.</i> ,	
	No. 17CV1718-LAB (WVG), 2018 WL 6018361 (S.D. Cal. Nov. 15, 2018)	9
	<i>Rhoades v. Avon Products, Inc.</i> ,	
	504 F.3d 1151 (9th Cir. 2007)	15

1	<i>Silver v. Stripe Inc.</i> ,	
2	No. 4:20-CV-08196-YGR, 2021 WL 3191752 (N.D. Cal. July 28, 2021).....	13
3	<i>Skaff v. Meridien N. Am. Beverly Hills, LLC</i> ,	
4	506 F.3d 832 (9th Cir. 2007)	6
5	<i>In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.</i> ,	
6	No. 3:19-CV-2284-H-KSC, 2020 WL 2214152 (S.D. Cal. May 7, 2020)	5
7	<i>Susinno v. Work Out World Inc.</i> ,	
8	862 F.3d 346 (3d Cir. 2017).....	14
9	<i>Svenson v. Google Inc.</i> ,	
10	No. 13-CV-04080-BLF, 2016 WL 8943301 (N.D. Cal. Dec. 21, 2016)	7, 8
11	<i>Svenson v. Google, Inc.</i> ,	
12	No. 13-CV-4080, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015)	8
13	<i>Thomas v. Unifin, Inc.</i> ,	
14	No. 21-cv-3037, 2021 WL 3709184 (N.D. Ill. Aug. 20, 2021)	11
15	<i>Transunion, LLC v. Ramirez</i> ,	
16	141 S. Ct. 2190 (2021).....	<i>passim</i>
17	<i>Travis v. Assured Imaging LLC</i> ,	
18	No. CV-20-00390-TUC-JCH, 2021 WL 1862446 (D. Ariz. May 10, 2021)	7, 8
19	<i>U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press</i> ,	
20	489 U.S. 749 (1989).....	12
21	<i>In re Uber Techs., Inc., Data Sec. Breach Litig.</i> ,	
22	No. CV182970PSGGJSX, 2019 WL 6522843 (C.D. Cal. Aug. 19, 2019)	8
23	<i>Van Patten v. Vertical Fitness Grp., LLC</i> ,	
24	847 F.3d 1037 (9th Cir. 2017)	14
25	<i>Verde v. Confi-Chek, Inc.</i> ,	
26	No. 21-cv-50092, 2021 WL 4264674 (N.D. Ill. Sept. 20, 2021).....	4
27	<i>In re Yahoo! Inc. Customer Data Security Breach Litig.</i> ,	
28	No. 16-MD-02752- LHK, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017).....	8
	<i>In re Zappos.com, Inc.</i> ,	
	888 F.3d 1020 (9th Cir. 2018)	5
	<i>Zevon v. American Express Co.</i> ,	
	No. 20-cv-4938, 2021 WL 4330578 (S.D.N.Y. Sept. 22, 2021)	4
	RULES	
	Rule 12(b)(1).....	15

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TREATISES

Restatement (Second) of Torts, § 652B (1977)12, 13

Restatement (Second) of Torts § 652D (1977) *passim*

1 I. INTRODUCTION

2 Plaintiffs’ claims for damages should be dismissed for lack of standing because neither of
 3 their asserted harms—the risk of identity theft and the mere compromise of their limited data in
 4 the Attack—qualifies as a concrete injury under *TransUnion*. Plaintiffs also lack standing for
 5 injunctive relief because any assertion that Zynga is at immediate risk of another data breach is
 6 sheer speculation, and in any event, Plaintiffs cannot show a successive breach would cause them
 7 harm any more than they can show harm from the Attack itself.

8 *First*, Plaintiffs acknowledge that *TransUnion* “rejected . . . the contention that the ‘risk
 9 of future harm’—on its own—serves as a basis for standing.” Opp’n to Mot. to Dismiss at 8
 10 (“Opp.”) (Dkt. 98). Yet Plaintiffs’ core argument for standing is based on just that—a purported
 11 risk of *future* identity theft or fraud. Plaintiffs allege no facts showing that they have *actually*
 12 had their identity stolen or been defrauded (let alone as a consequence of the Attack). *At most*,
 13 Plaintiffs allege *attempts* at account compromise or phishing; but they allege no facts to suggest
 14 that, at any time in the two years since the Attack, any such attempt succeeded and caused them
 15 harm. Plaintiffs’ characterization of those alleged attempts as evidence of a “present risk of
 16 harm” does not change the fact that no harm has ever materialized, and *TransUnion* makes clear
 17 that in a suit for damages, a risk of harm that has not materialized “cannot establish a concrete
 18 harm sufficient for standing.” *Transunion, LLC v. Ramirez*, 141 S. Ct. 2190, 2211 (2021).

19 *Second*, Plaintiffs’ argument that the exposure of their information in the Attack is, by
 20 itself, a “privacy” harm likewise ignores *TransUnion*’s strictures. *TransUnion* holds that for a
 21 harm to be concrete it must be “closely related” to the harm underlying a tort recognized under
 22 traditional common law. But the torts Plaintiffs rely upon—publicity given to private life and
 23 intrusion upon seclusion—require the disclosure of intimate facts about an individual’s personal
 24 life. The limited data at issue here—basic contact information, defunct passwords to an online
 25 word game, a telephone number and a birthdate—do not come close to meeting that description.
 26 Plaintiffs’ argument that the disclosure of *any* information relating to an individual constitutes an
 27 “invasion of privacy” would imply that *any* data breach automatically gives rise to standing, no
 28

1 matter how trivial the information involved. Such a rule would vastly *expand* standing in the
 2 data breach context rather than hewing to the limitations set forth in *TransUnion*.

3 *Third*, Plaintiffs have no basis for standing to seek injunctive relief. They offer no reason
 4 to believe that Zynga is at immediate risk of another data breach, but even if there were such an
 5 event, Plaintiffs would be just as unable to prove concrete harm as they are now. The same
 6 minimal information would still be at issue—even less so, since Zynga does not have any
 7 passwords created by Plaintiffs given the password reset it implemented after the Attack.

8 Plaintiffs have now had multiple chances to adequately plead concrete harm and have
 9 failed to do so. The Amended Complaint should therefore be dismissed without leave to amend.

10 **II. PLAINTIFFS' ALLEGATIONS BASED ON THE RISK OF FUTURE IDENTITY** 11 **THEFT DO NOT PROVIDE A BASIS FOR STANDING**

12 Plaintiffs attempt to rehash the same arguments regarding risk of future harm that this
 13 Court already found insufficient in dismissing the first consolidated Complaint (Dkt. 67). *See*
 14 Order Granting Mot. to Compel and Mot. to Dismiss at 3 (“MTD Order”) (Dkt. 93). Those
 15 arguments are foreclosed by *TransUnion* and should be rejected once again.

16 **A. *TransUnion* Forecloses Any Standing Argument Based on a Risk of Future** 17 **Harm**

18 Plaintiffs concede that, under *Transunion*, “injuries related to an ‘imminent risk’ of
 19 harm” do not confer standing unless that “risk of future harm materialize[s].” Opp. 2; *see also*
 20 *id.* 6 (stating that “the [Supreme] Court rejected the plaintiffs’ contention that the ‘risk of future
 21 harm’—on its own—serves as a basis for standing”). Yet, tellingly, Plaintiffs do not even *try* to
 22 explain how any alleged identity theft “risks” they identify have actually “materialized” into
 23 concrete harm. In particular, they make no attempt to engage with Zynga’s opening brief, which
 24 analyzed their allegations in detail—category-by-category and Plaintiff-by-Plaintiff—and
 25 explained how they are bereft of any actual instances of identity theft or fraud. Mot. to Dismiss
 26 Am. Compl. at 5-10 (“Mot.”) (Dkt. 96). Instead, Plaintiffs simply repeat those same allegations,
 27 which they expressly characterize as reflecting the *risk* of “credential stuffing” and “phishing
 28 scams” and supposed failed “attempts” at the same. Opp. 8. In fact, the Opposition references

1 “risk” or “risks” a total of 43 times, underscoring that Plaintiffs’ theory is based on the
 2 possibility of future injury—not any injury that has actually materialized.¹

3 Recognizing that *TransUnion* precludes any standing argument based on the mere risk of
 4 future harm, Plaintiffs try to distinguish its holding; but the distinctions they draw do not survive
 5 the slightest scrutiny.

6 First, Plaintiffs seek to distinguish *Transunion* because it “involved a fundamentally
 7 different type of alleged injury” than what Plaintiffs allege here—but that does not matter.
 8 *Transunion* establishes a legal rule that applies regardless of the specific injury alleged: “in a suit
 9 for damages, the mere risk of future harm . . . cannot qualify as a concrete harm.” 141 S. Ct. at
 10 2210-11. No matter what harm a plaintiff alleges, if the harm has not actually materialized then
 11 it cannot establish standing for damages. That legal rule forecloses standing here, because
 12 Plaintiffs rely exclusively on alleged risks of identity theft that have not materialized.

13 If anything, the difference in injuries alleged here versus in *Transunion* underscores why
 14 Plaintiffs’ allegations are insufficient. In *Transunion*, the Court found that the disclosure of
 15 credit reports “that labeled the class members as potential terrorists, drug traffickers, or serious
 16 criminals” could cause a “reputational harm associated with the tort of defamation,” 141 S. Ct. at
 17 2208-09 (emphasis added), which the Court found had not materialized for those class members
 18 whose credit reports were not actually disseminated. Here, Plaintiffs do not argue that the
 19 exposure of the information at issue has caused them any reputational harm. Instead, they point
 20 to the possibility that their information may in the future be used by third parties to commit
 21 identity theft. Opp. 5, 17. Thus, as with the plaintiffs the Court found *uninjured* in *Transunion*,
 22 the ultimate harm Plaintiffs claim to fear here—identity theft—has not actually materialized.

23
 24 ¹ Plaintiffs’ Opposition contains occasional perfunctory assertions that *actual* credential stuffing
 25 or unauthorized access has occurred, *see* Opp. 19, but Zynga has already explained that these
 26 assertions are merely hot air that are not actually supported by the Amended Complaint’s factual
 27 allegations. Mot. 6-8. Plaintiffs make no effort to rebut Zynga’s points and, revealingly, when it
 28 comes to stating their actual standing theory, they acknowledge that it is based on the “risk” of
 identity theft, not any supposed instance of identity theft that has actually occurred. *See* Opp. 8
 (stating that “Plaintiffs assert damages based on the actual misuse of their PII by cybercriminals
 attempting to commit identity theft and fraud—a present risk of harm” (emphasis altered)); *see*
 also *id.* at 9 (heading based on “Risk of Identity Theft and Fraud”).

1 Plaintiffs at most allege a *risk* of such harm, and *Transunion* unequivocally holds that a risk of
 2 future harm alone cannot establish standing.

3 *Second*, while Plaintiffs concede that *Transunion* “rejected the [] contention that the ‘risk
 4 of future harm’ . . . serves as a basis for standing,” they nonetheless argue that their allegations
 5 about “cybercriminals attempting to commit identity theft and fraud” show they face “a *present*
 6 risk of harm,” which they say provides a basis for standing. Opp. 7. But Plaintiffs’ effort to
 7 distinguish a “risk of future harm” from a “present risk of harm” is nonsensical. A present *risk* is
 8 nothing more than the possibility of *future* harm—which is exactly what *TransUnion* says is
 9 insufficient to establish standing. As *TransUnion* explains, a plaintiff may sue only if a “risk of
 10 future harm materializes and the individual suffers a concrete harm,” in which case “the harm
 11 itself, and *not the pre-existing risk*, will constitute a basis for the person’s injury and for
 12 damages.” 141 S. Ct. at 2211 (emphasis added).

13 *Third*, Plaintiffs remarkably argue that “*TransUnion* does not alter the landscape [] on a
 14 motion to dismiss,” but applies only in cases where there is a “record developed after full
 15 discovery and trial.” But Supreme Court opinions are not limited to the procedural posture in
 16 which they arise. Indeed, *TransUnion* itself makes clear that a plaintiff “must maintain their
 17 personal interest in the dispute *at all stages* of litigation.” *TransUnion*, 141 S. Ct. at 2208
 18 (emphasis added). Unsurprisingly, numerous courts have applied the principles in *TransUnion*
 19 to the motion to dismiss stage.² Plaintiffs cannot absolve themselves of the responsibility to
 20 establish standing at the pleading stage by speculating that they will somehow prove facts at trial
 21 that they cannot even truthfully *allege*.³

22
 23 ² See MTD Order at 3; *Zevon v. American Express Co.*, No. 20-cv-4938, 2021 WL 4330578, at
 24 *3-4 (S.D.N.Y. Sept. 22, 2021); *Iwaniv v. Early Warning Servs.*, No. 20-cv-5266, 2021 WL
 25 3209856, at *3 (E.D. Pa. July 28, 2021); *Verde v. Confi-Chek, Inc.*, No. 21-cv-50092, 2021 WL
 4264674, at *4-5 (N.D. Ill. Sept. 20, 2021); *Grauman v. Equifax Info. Servs.*, No. 20-cv-3152,
 2021 WL 3239865, at *5 (E.D.N.Y. July 16, 2021).

26 ³ The only authority Plaintiffs cite for limiting *TransUnion* to the post-trial context is
 27 unpersuasive dicta from in *In re Blackbaud, Inc., Customer Data Breach Litig.*, No. 20-MN-
 28 02972, 2021 WL 2718439, at *6 n.15 (D.S.C. July 1, 2021). There, after explaining that the
 defendant had “abandoned” its concrete injury argument, the court noted that it was “not in a
 position” to adjudicate the issue in any event because it was limited to the pleadings on a motion
 to dismiss. But nothing in *TransUnion* suggests that its principles do not apply with full force at

1 In short, Plaintiffs’ grounds for distinguishing *TransUnion* lack merit—and only serve to
 2 illustrate that their claims here rest on a *risk* of harm that has not in fact materialized. For that
 3 reason, Plaintiffs’ continued reliance on case law predating *TransUnion*—in particular, *In re*
 4 *Zappos.com, Inc.*, 888 F.3d 1020, 1023 (9th Cir. 2018) and *Krottner v. Starbucks Corp.*, 628
 5 F.3d 1139, 1143 (9th Cir. 2010) is misplaced. Plaintiffs cite these cases for the proposition that
 6 an “increased risk of identity theft constitutes an injury-in-fact,” Opp. 9, but that proposition is
 7 squarely at odds with *TransUnion*’s holding that the risk of future harm cannot supply standing
 8 to sue for damages. Any suggestion in *Zappos* or *Krottner* that such a risk supplies a basis for
 9 standing in a damages suit has been superseded by *TransUnion*’s holding.⁴

10 **B. Plaintiffs Cannot Manufacture Standing Based on Mitigation Efforts or**
 11 **Emotional Distress Allegedly Stemming from the Risk of Identity Theft**

12 Plaintiffs also rehash arguments that they previously made in their defense of the prior
 13 Complaint based on mitigation efforts they have allegedly taken and emotional distress they have
 14 allegedly experienced as a result of the Attack. These arguments remain meritless given the
 15 minimal information at issue.

16 **1. Mitigation Efforts**

17 Plaintiffs assert that loss of time spent “addressing the consequences” of a data breach
 18 constitutes an injury-in-fact, citing to cases finding standing where plaintiffs had to monitor
 19 financial accounts and credit reports for signs of identity theft. But those cases involved
 20 individuals who had sensitive financial and identification information exposed that could be
 21 directly used to make fraudulent payments or open new lines of credit. *See In re Solara Med.*
 22 *Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-CV-2284-H-KSC, 2020 WL
 23 2214152, at *1, 4 (S.D. Cal. May 7, 2020) (involving breach of financial information and social

24 the pleadings stage, and moreover Zynga is making a factual attack on standing here, so the
 Court can rely on facts outside the pleadings to the extent it deems necessary to do so.

25 ⁴ In any event, *Zappos* and *Krottner* are distinguishable on their own terms, because they
 26 involved the taking of sensitive financial and identification information, as this Court already
 27 noted. *See* MTD Order at 3 (distinguishing both cases); Mot. to Dismiss Hearing Tr. 13:17-20
 28 (“Tr.”) (Dkt. 94) (noting that “*Krottner* and *Zappos* involved . . . more sensitive information than
 [Plaintiffs have] alleged here”); *see also In re Zappos.com, Inc.*, 888 F.3d at 1023 (9th Cir. 2018)
 (credit card numbers); *Krottner*, 628 F.3d at 1140 (social security numbers). Plaintiffs provide
 no reason for this Court to reconsider its view now.

1 security numbers); *In re Experian Data Breach Litig.*, No. SACV151592AGDFMX, 2016 WL
 2 7973595, at *1, 5 (C.D. Cal. Dec. 29, 2016) (social security numbers); *In re Anthem, Inc. Data*
 3 *Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *2, 26 (N.D. Cal. May 27, 2016)
 4 (social security numbers, health care ID numbers, and income data); *Lewert v. P.F. Chang's*
 5 *China Bistro, Inc.*, 819 F.3d 963, 965, 967 (7th Cir. 2016) (debit and credit card data). No
 6 comparable information was taken here: Zynga does not even collect such sensitive information.
 7 Thus, Plaintiffs have no need to spend any time poring over financial statements, canceling credit
 8 cards, or obtaining credit monitoring—as in the cases they rely on.

9 As for Plaintiffs' reference to "time spent changing passwords," Zynga has already
 10 explained that using unique passwords on online accounts is "nothing more than the exercise of
 11 ordinary due diligence" that everyone should undertake, regardless of whether they have been
 12 subject to any data breach. Mot. 12 (citing *In re Equifax, Inc., Customer Data Sec. Breach*
 13 *Litig.*, No. 1:17-MD-2800-TWT, 2019 WL 926999, at *5 (N.D. Ga. Jan. 28, 2019)). Plaintiffs
 14 offer no explanation for their perfunctory assertion that their actions instead amount to
 15 "heightened diligence." Opp. 13. And, in any event, as this Court previously noted, changing a
 16 password takes "30 seconds," Tr. 14:24-15:7—an inconvenience "too trifling" to "support
 17 constitutional standing." *Skaff v. Meridien N. Am. Beverly Hills, LLC*, 506 F.3d 832, 839-40 (9th
 18 Cir. 2007). Unsurprisingly, Plaintiffs cite no case law holding that time spent changing
 19 passwords constitutes a concrete injury for purposes of standing, and there is no reason for this
 20 Court to set any such precedent here.

21 2. Emotional Distress

22 Next, in a single paragraph, Plaintiffs argue they have standing because they are suffering
 23 ongoing "stress" over the possibility that their information could someday be misused to harm
 24 them, notwithstanding the limited nature of the information affected in the Attack. Plaintiffs do
 25 not respond to Zynga's cited cases rejecting similar allegations as a basis for standing, *see* Mot.
 26 11, and their sole citation to *Krottner* is inapposite because that case involved much more
 27 sensitive information—including social security numbers. 628 F.3d at 1142. Moreover, to the
 28 extent Plaintiffs profess to be concerned about the risk of credential stuffing, those assertions are

inconsistent with their own allegations that they proactively changed their passwords on other accounts since the Attack—which would obviate any credential stuffing risk.⁵ Particularly given that more than two years have elapsed since the Attack without any Plaintiffs actually experiencing identity theft or fraud, Plaintiffs cannot manufacture standing for themselves simply by making vague and conclusory allegations that they fear a hypothetical harm. *See Travis v. Assured Imaging LLC*, No. CV-20-00390-TUC-JCH, 2021 WL 1862446, at *10 (D. Ariz. May 10, 2021) (rejecting similar allegations and noting that “time passing without harm actually occurring further undermines the claim that the threat of harm is immediate, impending, or otherwise substantial”). Indeed, were such allegations enough, any plaintiff could bootstrap their way into standing simply by alleging “stress” or other emotional injury. Mot. 11-12.

C. Plaintiffs Cannot Establish Standing Based on an Alleged “Loss of Value” in Their Information

Finally, Plaintiffs argue that they have standing because “their PII ha[s] inherent value, and that value was diminished as a result of the Data Breach.” Opp. 14. Their argument is no different from when they unsuccessfully made it to the Court in defending the prior Complaint. *See* Opp’n to Initial MTD at 8 (Dkt. 78). Plaintiffs still plead neither the “existence of a market for [their] personal information [nor] an impairment of [their] ability to participate in that market.” *Svenson v. Google Inc.*, No. 13-CV-04080-BLF, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016); *see also In re Google, Inc. Privacy Pol’y Litig.*, No. 5:12-CV-001382-PSG, 2015 WL 4317479, at *5 (N.D. Cal. July 15, 2015) (granting motion based on similar deficiencies in the plaintiffs’ allegations). Plaintiffs assert only that there must be a market for their information because “it was sold on multiple occasions to cybercriminals.” Opp. 14. But a *criminal* market is obviously not a market *Plaintiffs themselves* could or would ever participate in. Thus, whatever economic value Plaintiffs’ information might have to criminals seeking to illegally misappropriate it, that is not value that Plaintiffs could realize.

⁵ Plaintiffs hypothesize there may be some account they no longer remember on which they used their Zynga password, but this possibility—that maybe there is such an account, and maybe it contains some sort of sensitive information, and maybe a third party will attempt to and succeed in accessing it—is far too speculative a basis for standing. *See Clapper v. Amnesty Int’l*, 568 U.S. 398, 414 (2013) (rejecting standing theory based on “speculative chain of possibilities”).

1 The cases Plaintiffs cite (Opp. 14-15) are either distinguishable or unpersuasive, or both.
 2 Some do not discuss standing at all.⁶ In some that do, the courts *declined* to find standing based
 3 on loss of value of information, based on deficiencies similar to those here.⁷ Of the three cases
 4 Plaintiffs cite where standing was found based on loss of value, one involved specific allegations
 5 explaining the loss of economic value *to the plaintiff*, which is exactly what is lacking here.⁸ The
 6 other two⁹ are unpersuasive—they fail to explain how the data “lost value” for the plaintiff when
 7 there was no market for the data the plaintiff was alleged to participate in—and are outliers
 8 against the overall trend in the case law. Recent decisions consistently reject standing based on a
 9 “loss of value” theory where “[p]laintiffs have not alleged any facts explaining how their
 10 personal information became less valuable as a result of [a data breach] or that they attempted to
 11 sell their personal information [themselves, but] could not because of the [data breach].” *Travis*,
 12 2021 WL 1862446, at *9 (collecting cases).¹⁰

14 ⁶ See *In re Facebook Privacy Litigation*, 572 F. App’x 494, 494 (9th Cir. 2014); *In re Experian*
 15 *Data Breach Litig.*, No. SACV151592AGDFMX, 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29,
 2016).

16 ⁷ In *Hameed-Bolden v. Forever 21 Retail, Inc.*, the court *dismissed* the plaintiffs’ complaint,
 17 concluding that it “[f]ell short of demonstrating how Plaintiffs’ specific losses [related to loss of
 18 value in PII] constitute ‘property damages.’” No. CV1803019SJOJPRX, 2018 WL 6802818, at
 19 *5 (C.D. Cal. Oct. 1, 2018). Plaintiffs also cite *Svenson v. Google, Inc.*, No. 13-CV-4080, 2015
 20 WL 1503429, at *5 (N.D. Cal. Apr. 1, 2015), but the court in that case eventually held in a later
 opinion that the plaintiff had *not* shown “injury in fact based on diminution in value of her
 personal information,” because there was no showing of “a market for Svenson’s personal
 information or an impairment to her ability to participate in such a market resulting from
 Google’s alleged sharing of her personal information.” *Svenson*, 2016 WL 8943301, at *9.

21 ⁸ See *In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D.
 22 Md. 2020) (involving impairment of “the economic benefit the consumer derives from being able
 to purchase goods and services remotely and without the need to pay in cash or a check” because
 “[p]laintiffs allege[d] that they suffered lower credit scores as a result of the data breach and that
 fraudulent accounts and tax returns were filed in their names”).

23 ⁹ *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 865 (N.D. Cal. 2011); *In re Yahoo! Inc.*
 24 *Customer Data Security Breach Litig.*, No. 16-MD-02752- LHK, 2017 WL 3727318, at *13-14
 (N.D. Cal. Aug. 30, 2017).

25 ¹⁰ See also, e.g., *Dearing v. Magellan Health Inc.*, No. CV-20-00747-PHX-SPL, 2020 WL
 26 7041059, at *4 (D. Ariz. Sept. 3, 2020) (“[T]he Court agrees with decisions from the Northern
 District of California, which have been unwilling to find standing based solely on a theory that
 the value of a plaintiff’s PII has been diminished.” (citing cases)); *Bass v. Facebook, Inc.*, 394 F.
 27 Supp. 3d 1024, 1040 (N.D. Cal. 2019) (rejecting standing based on loss of value where plaintiff
 28 “has not shown how this information has economic value to him,” regardless of whether it “has
 external value” to others); *In re Uber Techs., Inc., Data Sec. Breach Litig.*, No.

III. PLAINTIFFS FAIL TO ALLEGE ANY PRIVACY INJURY WITH A CLOSE CONNECTION TO A COMMON LAW TORT

Plaintiffs assert that their alleged injuries are analogous to the torts of (1) publicity given to private life and (2) intrusion upon seclusion. But Plaintiffs do not dispute that disclosure of the minimal information at issue here would be insufficient to establish liability under either of these torts, both of which require disclosure of highly “intimate” facts. Instead, Plaintiffs argue that they “need not allege facts that exactly duplicate the elements of a common law claim.” Opp. 16. As *TransUnion* makes clear, however, while an “exact duplicate” is not required, a “close relationship” is. 141 S. Ct. at 2204, 2209. The Court was careful to note that this rule is a narrow one and “not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts.” *Id.* at 2204. Plaintiffs here ignore that admonition entirely. Their theory would turn *TransUnion* on its head and significantly *expand* standing in data breach cases, by permitting virtually any breach to qualify as an injury-in-fact, no matter how insignificant the information taken. That theory should be rejected out of hand.

A. Plaintiffs Fail to Allege an Injury with a Close Connection to the Tort of Publicity Given to Private Life

As Zynga has explained, the tort of publicity given to private life prohibits “publiciz[ing]” “a matter concerning the private life of another,” if that matter is “of a kind” that “would be highly offensive to a reasonable person” and “not of legitimate concern to the public.” Restatement (Second) of Torts § 652D (1977). “Private matters” include sexual relationships, family quarrels, humiliating illnesses, and intimate personal letters. Restatement (Second) of Torts § 652D cmt. b. In other words, the facts disclosed must be “*intimate details* of plaintiffs’ lives,” *Karimi v. Golden Gate Sch. of L.*, 361 F. Supp. 3d 956,980 (N.D. Cal. 2019), *aff’d*, 796 F.

CV182970PSGGJSX, 2019 WL 6522843, at *5 (C.D. Cal. Aug. 19, 2019) (“loss of value of ... private information” is “too abstract and speculative to support Article III standing”); *Razuki v. Caliber Home Loans, Inc.*, No. 17CV1718-LAB (WVG), 2018 WL 6018361, at *1 (S.D. Cal. Nov. 15, 2018) (plaintiff “fail[ed] to allege enough facts to establish how his personal information is less valuable as a result of [data] breach”); *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1088–89 (E.D. Cal. 2015) (failure to allege market for data and impairment of plaintiff’s ability to participate in that market is fatal to standing).

App’x 462 (9th Cir. 2020), disclosure of which “would be not merely embarrassing and painful but deeply shocking to the average person subjected to such exposure.” *Chisholm v. Foothill Capital Corp.*, 3 F. Supp. 2d 925, 941 (N.D. Ill. 1998); see *Ignat v. Yum! Brands, Inc.*, 214 Cal. App. 4th 808, 820-21 (2013) (disclosure would “shock the community’s notions of decency”).

The information at issue here—screen names, email addresses, phone number and birthday (for one Plaintiff), and passwords for an online word game (for two Plaintiffs)¹¹—does not come close to meeting this standard. Screen names are by their nature public—they are how Plaintiffs would have appeared on Zynga games they played. Email addresses and phone numbers are mere contact information that do not reveal “intimate details” about anyone’s private life. No one would claim, for example, that details found in a phone book are “intimate.” As for birthday, the Restatement itself makes clear that there is no liability for “giving publicity to facts about the plaintiff’s life that are matters of public record, such as the date of his birth.” Restatement (Second) of Torts § 652D cmt b. Nor is a password, particularly for *an online word game*, an “intimate detail” whose exposure would be “deeply shocking” to an ordinary person. While a password may provide a key to information that is sensitive, the password in and of itself reveals nothing about an individual’s private life.¹²

Plaintiffs do not try to contend that the information at issue would actually satisfy the elements of publicity given to private life; instead, they argue that it is “sufficiently analogous.” But the cases Plaintiffs cite for that proposition only further undermine their argument. Plaintiffs primarily rely on *Hunstein v. Preferred Collection & Mgmt. Servs.*, 994 F.3d 1341, 1347 (11th Cir. 2021), but there the disclosure involved the plaintiff’s “outstanding balance [on a debt], the

¹¹ Plaintiffs repeatedly try to muddy the waters concerning the types of data taken with respect to Plaintiffs in the Attack, asserting at points that the data included “Facebook login credentials” and “geolocation” data (Opp. 21), and Rosiak’s Facebook name, user ID, and phone number (Opp. 3). As Zynga has explained, these *ipse dixit* assertions are baseless and unsupported by any competent evidence to rebut the Ferris Declaration, which is the only admissible evidence in the record concerning the information taken in the Attack. Mot. 8 n.6.

¹² Plaintiffs do not allege that any intimate information was held in their Zynga account, or that those accounts were ever accessed. Instead, they once again generally point (Opp. 23) to the *risk* that hackers could “obtain additional confidential information contained in the Plaintiffs’ email accounts and other locations where they used the same login credentials.” But that simply brings Plaintiffs back to the problem of relying on future harm as a basis for standing.

fact that his debt resulted from his son’s medical treatment, and his son’s name.” *Id.* at 1344. Information regarding an individual’s personal debt and child’s medical treatment is, of course, much closer to an intimate detail of one’s private life than any of the types of data at issue here.¹³ Plaintiffs also rely on *Davis v. Facebook, Inc. (In re Facebook Inc. Internet Tracking Litig.)*, 956 F.3d 589, 598-99 (9th Cir. 2020), but the information alleged to be disclosed there consisted of “a great deal of personalized information” forming “a cradle-to-grave profile” of a person’s life. *Id.* at 599; *see id.* at 598-99, 605 (defendant tracked users’ browser history “no matter how sensitive” the websites visited, which “could divulge a user’s personal interests, queries, and habits,” and aggregated with information in user profiles, including employment history and political and religious affiliations). By contrast, Plaintiffs here do not allege any similarly sensitive information was exposed in the Attack, or even collected by Zynga in the first place.¹⁴

Plaintiffs also have no serious response to Zynga’s argument that Plaintiffs have not alleged the “publicity” of the allegedly private information. Plaintiffs again argue that the information has been “publicized to cyber criminals and is accessible on the internet” via the “Dark Web.” Opp. 23. But disclosure to a group of criminals on an illegal platform is not disclosure to “the public at large.” Restatement (Second) of Torts § 652D cmt. a (explaining that “publicity” as used in § 652D “differs from ‘publication,’ as that term is used in § 577 in connection with liability for defamation”).

Unable to show a “close relationship” to the essential elements of this tort, Plaintiffs try to rewrite the tort itself. In Plaintiffs’ telling, the tort of publicity given to private life is not

¹³ Plaintiffs assert (Opp. 20) that the court in *Hunstein* “did not consider whether the information disclosed was embarrassing or intimate.” But that is simply false. The court in *Hunstein* recited the Restatement’s clear requirement that “the matter publicized is of a kind that would be highly offensive to a reasonable person,” 994 F.3d at 1347. There is no indication that *Hunstein* would have found injury if that threshold requirement had not been met.

¹⁴ Both *Hunstein* and *Davis* also involved harms that Congress had chosen to “elevate” into statutory causes of action, *see TransUnion*, 141 S. Ct. at 2205, unlike here. The other cases Plaintiffs’ cite for this proposition similarly involve information much more sensitive than the information alleged here, and a statutory cause of action. *See Keller v. Northstar Location Servs.*, No. 21-cv-3389, 2021 WL 3709183, at *1 (N.D. Ill. Aug. 20, 2021) (FDCPA case involving disclosure of plaintiffs’ “names and addresses, their status as debtors, their alleged debts, and other personal information”); *Thomas v. Unifin, Inc.*, No. 21-cv-3037, 2021 WL 3709184, at *1 (N.D. Ill. Aug. 20, 2021) (FDCPA case involving disclosure of debt information).

1 about the revelation of intimate details, but rather about an individual’s “control of information
 2 concerning his or her person.” Opp. 20. And under that logic, Plaintiffs contend, the exposure of
 3 *any* information about a person—even non-intimate information such as an email address or a
 4 screen name—qualifies as an injury, because the person has lost “control” over it. That novel re-
 5 characterization would come as a surprise to the writers of the Restatement. As the Restatement
 6 expressly recognizes, this tort is based on the intimacy of the information itself. Restatement
 7 (Second) of Torts, § 652D, cmt. b (tort liability exists when “intimate details of [plaintiff’s]
 8 life”—such as “[s]exual relations” or “humiliating illnesses”—“are spread before the public gaze
 9 in a manner highly offensive to the ordinary reasonable man”). Plaintiffs rely on language from
 10 *U.S. Dep’t of Just. v. Reps. Comm. For Freedom of Press*, but that case (which, in any event, did
 11 not directly discuss this tort) involved disclosure of an individual’s FBI “rap sheet,” which is
 12 obviously intimate information. 489 U.S. 749, 762 (1989) (noting the “web of federal statutory
 13 and regulatory provisions that limits the disclosure of rap-sheet information”). *Reporters*
 14 *Committee* thus plainly does not support Plaintiffs’ expansive theory that “loss of control” of *any*
 15 information—regardless of its intimacy—constitutes Article III injury. Plaintiffs’ last-ditch
 16 effort to re-define this tort only underscores that they have failed to alleged an injury with a close
 17 connection to how the tort would be understood at common law.

18 **B. Plaintiffs Fail To Allege an Injury with a Close Relationship to the Tort of**
 19 **Intrusion Upon Seclusion**

20 The common law tort of intrusion upon seclusion requires a plaintiff to show a “highly
 21 offensive, intentional intrusion by the defendant into either (1) the plaintiffs’ “solitude or
 22 seclusion,” or (2) “his private affairs or concerns.” Restatement (Second) of Torts, § 652B.
 23 While Plaintiffs’ Opposition is less than clear as to what sort of “intrusion upon seclusion” they
 24 are referring to, the only reference to “intrusion upon seclusion” in the factual allegations of the
 25 Amended Complaint concern the hypothetical possibility that Plaintiffs’ Zynga passwords will
 26 be used to obtain access to their email accounts or other accounts containing information about
 27 their private affairs. See Am. Compl. ¶¶ 99 & n.48 (stating that “credential stuffing invades the
 28

1 privacy of the Plaintiffs and Class Members by intruding into their private matters and private
2 accounts” and citing to the Restatement section on “intrusion upon seclusion”).

3 This invocation of a privacy tort suffers from the same problem as Plaintiffs’ arguments
4 based on the risk of future identity theft. Putting conclusory rhetoric aside, Plaintiffs at most
5 allege only *attempts* to engage in “credential stuffing” (specifically, I.C. does, with respect to
6 other *gaming* accounts). None of the Plaintiffs allege that anyone actually *succeeded* in
7 obtaining access to their email account or the contents of any other account containing
8 information about their private affairs. Thus, they have no basis to assert that any such private
9 affairs have been “intruded” upon. Again, Plaintiffs cannot avoid the effect of *TransUnion* by
10 alleging the *risk* of an intrusion upon seclusion: so long as that harm has not materialized, it
11 cannot serve as the basis for standing any more than any other future harm.¹⁵

12 To the extent Plaintiffs are arguing that unwanted emails or calls they have allegedly
13 received are themselves an intrusion upon seclusion, that argument too is unpersuasive. As an
14 initial matter, Plaintiffs did not allege that those emails or calls were an intrusion on seclusion in
15 their Amended Complaint. *See Silver v. Stripe Inc.*, No. 4:20-CV-08196-YGR, 2021 WL
16 3191752, at *7 (N.D. Cal. July 28, 2021) (citation omitted) (a “complaint may not be amended
17 by briefs in opposition to a motion to dismiss.”) But in any event, unsolicited communications
18 only constitute an “intrusion upon seclusion” where they are “repeated with such persistence and
19 frequency as to amount to a course of hounding” that is “a substantial burden [on] existence.”
20 Restatement (Second) of Torts § 652B cmt. d. Plaintiffs’ allegations do not come close to
21 meeting this steep threshold. Receiving unsolicited emails does not create any “substantial
22 burden on existence,” since they can easily be ignored or deleted. Plaintiffs cite no authority
23 suggesting that a secluded place is intruded whenever an unsolicited email is delivered to an

24 ¹⁵ Nor can the mere exposure of the information here constitute an intrusion upon seclusion. To
25 cause injury under this tort, invasions into “private concerns or concerns” must involve intimate
26 personal facts. *See* Restatement (Second) of Torts § 652B cmt b (invasion into “private
27 concerns” relates to “personal documents,” “private and personal mail,” or “private bank
28 account”); *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1018 (Ill. App. Ct. 2004) (plaintiff had not
met “private matter or private facts” requirement of the tort because information at issue was not
“facially revealing, compromising or embarrassing”). And, as discussed above, no such intimate
details have been disclosed here.

1 inbox, which is a routine aspect of modern life. *See Jackson v. Loews Hotels, Inc.*, No.
 2 EDCV18827DMGJCX, 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) (“[R]eceiving spam
 3 or mass mail does not constitute an injury.”); *Burgess v. Eforce Media, Inc.*, No. 1:07-cv-231,
 4 2007 WL 3355369, at *6 (W.D.N.C. Nov. 9, 2007) (no standing based on “frustration” of
 5 “unwanted and unwelcomed emails”).¹⁶ As for unwanted phone calls, Johnson is the *only*
 6 Plaintiff who had a phone number compromised in the Attack in the first place, Declaration of
 7 Jessup Ferris (“Ferris Decl.”) (Dkt. 72-12) ¶ 16, and she does not allege receiving any unsolicited
 8 calls, let alone any calls with such frequency as to constitute a “substantial burden on her
 9 existence.” *Cf. Oppenheim v. I.C. Sys., Inc.*, 695 F. Supp. 2d 1303, 1310 (M.D. Fla.), *aff’d*, 627
 10 F.3d 833 (11th Cir. 2010) (“thirty-five to forty telephone calls to [the plaintiff’s] residence over a
 11 period of approximately three months,” while “annoying and bothersome,” “did not rise to the
 12 requisite level of outrageous and unacceptable conduct contemplated by the tort of invasion of
 13 privacy based on intrusion”).¹⁷

14 **IV. PLAINTIFFS LACK STANDING FOR THEIR INJUNCTIVE RELIEF CLAIM**

15 Plaintiffs can have standing for injunctive relief only if they can show a “real and
 16 immediate threat of repeated injury” that an injunction would redress. *O’Shea v. Littleton*, 414
 17 U.S. 488, 496 (1974). Plaintiffs request an injunction here purportedly to prevent another attack
 18 on Zynga’s systems. But, despite peppering their Opposition with several false assertions about
 19 Zynga’s security measures—such as their misleading claim that Zynga has “admitted” “that its

21 ¹⁶ Indeed, I.C., who includes the most detailed allegations relating to email, identifies only two
 22 spam emails he received (*see id.* ¶¶ 107, 111), and admits he did not “check his email address on
 a regular basis” in any event, *id.* ¶ 110.

23 ¹⁷ Nor do Plaintiffs bring claims under any statute that might elevate the receipt of unsolicited
 24 emails or calls to a cognizable harm. *Cf. Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 463 (7th
 25 Cir. 2020) (recognizing that unsolicited calls and text messages “may be too minor an annoyance
 to be actionable at common law” and thus insufficient for standing, *unless* Congress has
 26 specifically chosen “to make [that] harm legally cognizable” through a statutory cause of action,
 like the Telephone Consumer Protection Act (TCPA)); *see also Van Patten v. Vertical Fitness*
 27 *Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (emphasizing importance of Congress’s
 judgment in “elevating” “injuries previously *inadequate in law*” to cognizable injuries by statute,
 including through the TCPA) (emphasis added); *Susinno v. Work Out World Inc.*, 862 F.3d 346,
 352 (3d Cir. 2017) (holding that, with TCPA, Congress “elevated a harm” that was “‘previously
 28 inadequate in law’” (citation omitted)).

1 systems were vulnerable to attack,” Opp. 1¹⁸—Plaintiffs do not allege any facts suggesting that
 2 Zynga faces any “real and immediate” threat of a successive breach, nor could they plausibly do
 3 so given that more than two years has elapsed and no such successive breach has occurred.

4 Regardless, Plaintiffs cannot claim they face any threat of *harm* from the prospect of a
 5 successive breach, even if one were to occur. They acknowledge that they have stopped playing
 6 Zynga games, which means they have not given Zynga any *new* information that was not already
 7 exposed during the Attack. *See* Am. Compl. ¶¶ 8, 17, 29, 32. Thus any hypothetical successive
 8 attack would only mean that the *same* (minimal) information that has *already* been exposed
 9 could be exposed again. Opp. 25. Plaintiffs fail to offer any explanation as to how, without an
 10 injunction, they would face any additional harm from something that has already happened. It
 11 layers speculation upon speculation to suggest that information that is purportedly *already*
 12 available to criminals on the “Dark Web” and caused no actual injury will somehow cause
 13 Plaintiffs harm if it is exposed a second time in some future data breach.¹⁹

14 The claim for injunctive relief should accordingly be dismissed for lack of standing.²⁰

15 **V. CONCLUSION**

16 For all of the foregoing reasons, the Court should grant Zynga’s Motion to Dismiss, and
 17 dismiss Plaintiffs’ Amended Complaint without leave to amend.

18 ¹⁸ The Securities and Exchange Commission filing on which Plaintiffs rely merely lists hacking
 19 attacks as a “Risk Factor” that Zynga faces as a leading provider of online social games. Zynga
 20 Form 10-K, Fiscal Year Ended December 31, 2012, at 11, 15-16,
 21 <https://www.sec.gov/Archives/edgar/data/1439404/000119312513072858/d489727d10k.htm>.
 Nothing in that filing suggests that Zynga’s security procedures were “outdated,” and Zynga’s
 general acknowledgment of risk factors cannot otherwise be construed as an admission.

22 ¹⁹ Indeed, even *less* information would be exposed in any successive attack, because Zynga reset
 23 all passwords affected in the Attack, Ferris Decl. ¶ 18, which Plaintiffs do not dispute. Plaintiffs
 24 argue that “Zynga asks this Court to make a merits determination that changing the passwords on
 25 affected Zynga accounts was enough to prevent further breach.” *Id.* at 25. But the password
 reset issue does not go to the merits. It goes to whether Plaintiffs would suffer concrete harm
 even in the event of another breach. Given that any Zynga passwords Plaintiffs had used
 previously would have been deleted from their accounts by the reset, Plaintiffs cannot claim they
 face any continuing threat that those passwords might be exposed in a future breach.

26 ²⁰ Plaintiffs claim that Zynga does not dispute its claim for declaratory relief. That is false. A
 27 plaintiff must either have been injured or be likely to suffer an imminent injury redressable by an
 28 injunction to have standing to bring a declaratory relief claim. *Rhoades v. Avon Products, Inc.*,
 504 F.3d 1151, 1157 (9th Cir. 2007) (“Absent a true case or controversy, a complaint solely for
 declaratory relief under 28 U.S.C. § 2201 will fail for lack of jurisdiction under Rule 12(b)(1).”).

1 DATED: October 12, 2021

LATHAM & WATKINS LLP

2 /s/ Elizabeth L. Deeley

3 Elizabeth L. Deeley (CA Bar No. 230798)

4 *elizabeth.deeley@lw.com*

5 505 Montgomery Street, Suite 2000

6 San Francisco, California 94111-6538

7 Telephone: +1.415.391.0600

8 Facsimile: +1.415.395.8095

9 Susan E. Engel (*pro hac vice*)

10 *susan.engel@lw.com*

11 555 Eleventh Street, N.W., Suite 1000

12 Washington, D.C. 20004-1304

13 Telephone: +1.202.637.2200

14 Facsimile: +1.202.637.2201

15 Serrin Turner (*pro hac vice*)

16 *serrin.turner@lw.com*

17 1271 Avenue of the Americas

18 New York, NY 10020

19 Telephone: +1.212.906.1200

20 Facsimile: +1.212.751.4864

21 Attorneys for Defendant Zynga Inc.